

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-191761

(43)Date of publication of application : 13.07.1999

(51)Int.Cl.

H04L 9/32

G09C 1/00

(21)Application number : 09-357158

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 25.12.1997

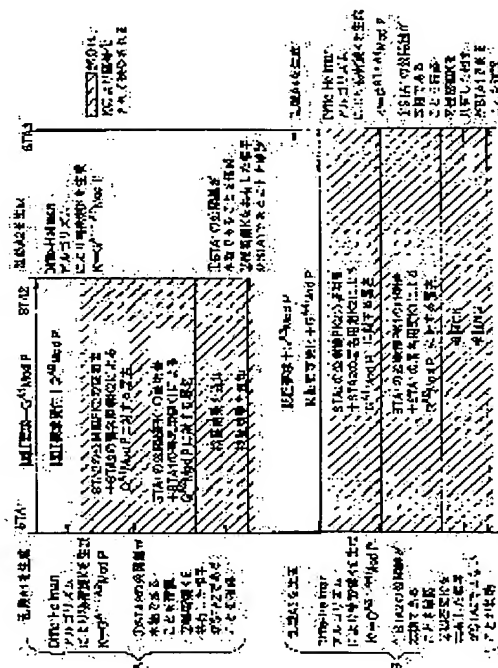
(72)Inventor : KUNO YUTAKA
KOBAYASHI TETSUTARO
MORITA HIKARI

(54) MUTUAL AUTHENTICATION METHOD AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mutual authentication method that keeps security against attacks and executes efficient authentication.

SOLUTION: A random number A1 is generated in a STAB, a GA1Mod P is sent to a SAT 2 by the Diffie-Hellman key delivery algorithm. The STA2 generates a random number A2 and sends GA2Mod P to the STA1. The STA1, STA2 obtain a shared key GA1.A2Mod P. The STA2 sends a certificate of a public key PK2 of the STA2 by an authentication station and a signature C2 of the GA1Mod P by a private key K2 to the STA1. The STA1 sends a certificate of a public key PK1 of the STA1 by an authentication station and a signature C1 of the GA2Mod P by a private key K1 to the STA2. The STA1, STA2 confirm the legitimacy of the public key based on the received information and authenticates the signatures with each other by using the respective public keys.



LEGAL STATUS

[Date of request for examination]

14.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3253060

[Date of registration]

22.11.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

特開平11-191761

(43) 公開日 平成11年(1999) 7月13日

(51) IntCl.⁶
H 0 4 L 9/32
G 0 9 C 1/00

識別記号
6 4 0

FI

H 0 4 L 9/00
C 0 9 C 1/00
H 0 4 L 9/00

6 7 5 B
6 4 0 E
6 4 0 B
6 7 5 D

審査請求 未請求 請求項の数7 OL (全11頁)

(21) 出願番号 特願平9-357158
(22) 出願日 平成9年(1997)12月25日

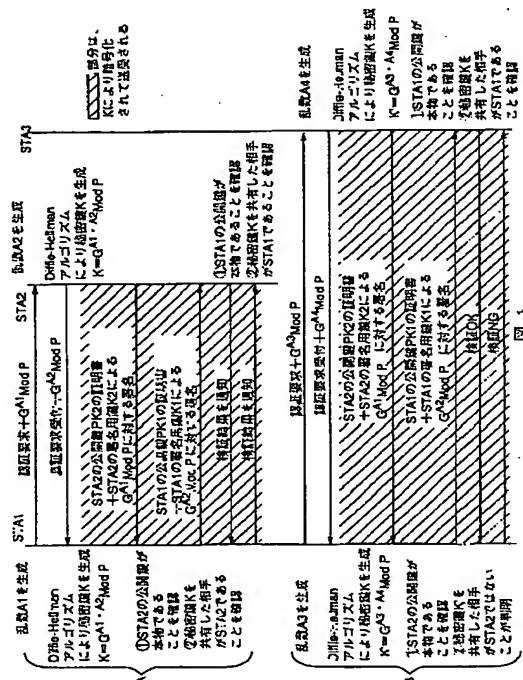
(71) 出願人 000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号
(72) 発明者 久埜 豊
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(72) 発明者 小林 鉄太郎
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(72) 発明者 森田 光
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(74) 代理人 弁理士 草野 卓

(54) 【発明の名称】 相互認証方法及びその装置

(57) 【要約】

【課題】 攻撃に対して安全であり、かつ効率的に行うことができる。

【解決手段】 STA1で乱数A1を生成し、Diffie-Hellman鍵配送アルゴリズムにより $G^{A1} \text{Mod } P$ をSTA2へ送り、STA2ではA2を生成し、 $G^{A2} \text{Mod } P$ をSTA1へ送り、STA1、STA2で共有鍵 $G^{A1 \cdot A2} \text{Mod } P$ を得る。STA2はSTA2の公開鍵PK2の認証局による証明書とその秘密鍵K2による $G^{A1} \text{Mod } P$ に対する署名C2をSTA1へ送り、STA1はその公開鍵PK1の証明書とその署名用鍵K1による $G^{A2} \text{Mod } P$ に対する署名C1をSTA2へ送る。各STA1、STA2では受信情報から、その公開鍵の正当性を確認し、かつその公開鍵で署名を検証する。



【特許請求の範囲】

【請求項1】 2台の通信装置STA1、STA2の一方の通信装置STA1が乱数A1を発生し、関数Fによって、 $F(A1)$ を算出して $F(A1)$ を他方の通信装置STA2に送信し、

通信装置STA2が乱数A2を発生し、関数Gによって、 $G(A2)$ を算出して $G(A2)$ を通信装置STA1に送信し、

通信装置STA1は乱数A1と、受信した $G(A2)$ から秘密鍵SKを生成し、

通信装置STA2は乱数A2と、受信した $F(A1)$ から秘密鍵SKを生成し、

共有した秘密鍵SKを用いた暗号通信を行う通信システムにおける相互認証方法において、

通信装置STA1は、

① 通信装置STA1のデジタル署名用鍵K1に対応する公開鍵PK1

② 認証局によるPK1へのデジタル署名B1（以下、公開情報PIと、認証局によるPIに対するデジタル署名の組のことを、PIの証明書と呼ぶ。①と②はSTA1の公開鍵PK1の証明書S1である。）

③ $G(A2)$ の通信装置STA1の署名用鍵K1によるデジタル署名C1

を通信装置STA2に送信し、

通信装置STA2は

④ 通信装置STA2のデジタル署名用鍵K2に対応する公開鍵PK2の証明書S2

⑤ $F(A1)$ の通信装置STA2の署名用鍵K2によるデジタル署名C2

を通信装置STA1に送信し、通信装置STA1、STA2でそれぞれ受信した証明書とデジタル署名の検証を行うことを特徴とする相互認証方法。

【請求項2】 上記 $G(A2)$ の署名用鍵K1によるデジタル署名C1は、 $G(A2)$ を変数とする関数 $H(G(A2))$ に対するK1によるデジタル署名であり、

上記 $F(A1)$ の署名用鍵K2によるデジタル署名C2は、 $F(A1)$ を変数とする関数 $I(F(A1))$ に対するK2によるデジタル署名であることを特徴とする請求項1記載の相互認証方法。

【請求項3】 上記関数Hの変数として、上記乱数A1を含み、上記関数Iの変数として上記乱数A2を含むことを特徴とする請求項2記載の相互認証方法。

【請求項4】 2台の通信装置STA1、STA2の一方の通信装置STA1が公開鍵 α を他方の通信装置STA2に送信し、

通信装置STA2が乱数A2を発生し、関数Gによって、 $G(\alpha, A2)$ を算出して $G(\alpha, A2)$ を通信装置STA1に送信し、

通信装置STA1は、 $G(\alpha, A2)$ から秘密鍵SKを生成し、通信装置STA2はA2から秘密鍵SKを生成

し、

共有した秘密鍵SKを用いた暗号通信を行う通信システムにおける相互認証方法において、

通信装置STA1は乱数A1を発生し、

① 通信装置STA1のデジタル署名用鍵K1に対応する公開鍵PK1の証明書S1

② $(A1, G(\alpha, A2))$ の通信装置STA1の署名用鍵K1によるデジタル署名C1

③ 乱数A1

を通信装置STA2に送信し、

通信装置STA2は

④ 通信装置STA2のデジタル署名用鍵K2に対応する公開鍵PK2の証明書S2

⑤ 関数Iを用いて算出される $(A1, G(\alpha, A2))$ の通信装置STA2の署名用鍵K2によるデジタル署名C2

を通信装置STA1に送信し、通信装置STA1、STA2でそれぞれ受信した証明書とデジタル署名の検証を行うことを特徴とする相互認証方法。

【請求項5】 上記 $(A1, G(\alpha, A2))$ に対する署名用鍵K1によるデジタル署名C1は、 $(A1, G(\alpha, A2))$ を変数とする関数 $H(A1, G(\alpha, A2))$ に対するK1による署名であり、

上記 $(A1, G(\alpha, A2))$ に対する署名用鍵K2によるデジタル署名C2は、 $(A1, G(\alpha, A2))$ を変数とする関数 $I(A1, G(\alpha, A2))$ に対するK2による署名であることを特徴とする請求項4記載の相互認証方法。

【請求項6】 乱数 A_n 、共有秘密鍵SK、認証用公開鍵 PK_n の認証局の証明書、公開鍵 PK_n と対応する署名用秘密鍵 K_n 、相手通信装置から共有鍵配送時に受信した鍵配送用関数値 $G(A_i)$ を記憶する記憶手段と、

上記乱数 A_n を生成する乱数生成手段と、

上記乱数 A_n を変数とする関数演算を行う鍵配送用演算手段と、

相手通信装置からの鍵配送用関数値 $G(A_i)$ と乱数 A_n とを用いて上記共有の秘密鍵SKを生成する共有鍵生成手段と、

上記鍵配送用関数値 $G(A_i)$ に対し上記署名用秘密鍵 K_n によるデジタル署名 C_n を生成する署名手段と、

相手通信装置からの公開鍵 PK_i に対する証明書からその公開鍵 PK_i の正当性を確認する公開鍵確認手段と、

上記相手通信装置からの鍵配送用関数値 $G(A_n)$ に対する署名 C_i を上記公開鍵 PK_i で検証する署名検証手段と、

上記公開鍵確認手段の確認結果と、上記署名検証手段の検証結果とから相互認証に対する検証結果を生成する手段と、

上記鍵配送用演算手段の演算結果 $F(A_n)$ 、上記署名 C_n および上記公開鍵 PK_n の証明書、上記認証結果を

上記相手通信装置へ送信する送信手段と、
外部からの情報を受信する受信手段と、
上記各手段を制御し、順次処理を実行させる制御手段と
を具備する相互認証用通信装置。

【請求項7】 鍵配送用公開鍵及び秘密鍵、相手通信装置からの暗号関数値 $G(\alpha, A_i)$ と乱数 A_n 、共有秘密鍵 SK 、認証用公開鍵 PK_n の証明書 S_n 、その PK_n と対応する署名用秘密鍵 K_n を記憶する記憶手段と、
鍵配送用乱数 A_n を生成する乱数生成手段と、
相手通信装置からの公開鍵 β により上記乱数 A_n を暗号化して暗号関数値 $G(\beta, A_n)$ を得る暗号手段と、
相手通信装置からの暗号関数値 $S_i = G(\alpha, A_i)$ と上記鍵配送用公開鍵 α とを入力して、上記共有鍵 SK を生成する共有鍵生成手段と、
認証用乱数 A_n' を生成する乱数生成手段と、
上記認証用乱数 A_n' と、上記相手通信装置からの暗号関数値 S_i に対する上記署名用秘密鍵 K_n によりデジタル署名 C_n を生成する署名手段と、
相手通信装置からの公開鍵 PK_i に対する証明書からその公開鍵 PK_i の正当性を確認する公開鍵確認手段と、
上記相手通信装置からの暗号関数値 $G(\alpha, A_i)$ と乱数 A_n' に対する署名 C_i を上記公開鍵 PK_i で検証する署名検証手段と、
上記公開鍵確認手段の確認結果と、上記署名検証手段の検証結果とから相互認証に対する検証結果を生成する手段と、
上記鍵配送用公開鍵 α 、上記暗号関数値 $G(\beta, A_n)$ 、上記証明書 S_n 及び署名 C_n 、上記相互認証検証結果を相手通信装置に送信する送信手段と、
外部からの情報を受信する受信手段と、
上記各手段を制御し、順次処理を実行させる制御手段とを具備する相互認証用通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信により共通の秘密鍵を生成し、その秘密鍵により暗号通信を行う通信システムにおける通信相手の相互認証方法及びその装置に関する。

【0002】

【従来の技術】以下では、署名とは、デジタル署名を意味する。従来の相互認証方法にはX5056-3 (ISO/IEC9798-3) 5.2 Mutual Authentication (相互認証) に定める相互認証プロトコルがあった。そのおもなプロトコルとしては、以下の2つがある。

・ 5.2.1 Two Pass Authentication

・ 5.2.2 Three Pass Authentication

また、相互認証プロトコルに対する主な攻撃（なりすまし）として、

・ Man in the Middle 攻撃

・ Replay攻撃

がある。

【0003】まず、この従来の相互認証方法の概要を示す。

(1) 5.2.1 Two Pass Authentication

図7AにTwo Pass Authentication の概要を示す。

1：通信装置STA1は相互認証プロトコルをおこなう時点の時刻を $T1$ とし、 $[T1, STA2]$ に対する署名 $S1$ を生成する。

2：通信装置STA1は通信装置STA1の公開鍵 $PK1$ の証明書（ $PK1$ と $PK1$ に対する認証局の署名 $B1$ ）と $T1, STA2, S1$ とを通信装置STA2へ送る。（図7Aの1）

3：通信装置STA2は通信装置1からSTA1の証明書 $B1$ を用いて署名 $S1$ を検査し、検査に不合格の場合はプロトコルを中断する。

4：通信装置STA2はプロトコルをおこなう時点の時刻を $T2$ とし、 $[T2, STA1]$ に対する署名 $S2$ を生成する。

5：通信装置STA2は通信装置STA2の公開鍵 $PK2$ の証明書（ $PK1$ とその署名 $B2$ ）、 $T2, STA1, S2$ を通信装置STA1へ送る。（図7Aの2）

6：通信装置STA1は通信装置STA2からの証明書をを用いて署名 $S2$ を検査し、検査に不合格の場合はプロトコルを中断する。

【0004】3、6の検査が両方とも合格だった場合に、相互認証が成立する。

(2) 5.2.2 Three Pass Authentication

図7BにThree Pass Authentication の概要を示す。

1：通信装置STA2は乱数 $R2$ を生成し、通信装置STA1へ送る。（図7Bの1）

2：通信装置STA1は乱数 $R1$ を生成し、 $[R1, R2, STA2]$ に対する署名 $S1$ を生成する。

3：通信装置STA1はその公開鍵 $PK1$ の証明書、 $R1, R2, STA2, S1$ を通信装置STA2へ送る。（図7Bの2）

4：通信装置STA2は通信装置STA1からの証明書をを用いて署名 $S1$ を検査し、検査に不合格の場合はプロトコルを中断する。

5：通信装置STA2は $[R2, R1, STA1]$ に対する署名 $S2$ を生成する。

6：通信装置STA2はその公開鍵 $PK2$ の証明書、 $R2, R1, STA1, S2$ を通信装置STA1へ送る。（図7Bの3）

7：通信装置STA1は通信装置STA2からの証明書をを用いて署名 $S2$ を検査し、検査に不合格の場合はプロトコルを中断する。

【0005】4、7の検査が両方とも合格だった場合に、相互認証が成立する。上記で説明した、従来の認証プロトコル

- ・ 5. 2. 1 Two Pass Authentication
- ・ 5. 2. 2 Three Pass Authentication

では、以下に説明するReplay攻撃を防ぐことはできるが、Man in the Middle 攻撃を防ぐことはできないという問題点がある。

・ Man in the Middle 攻撃

通信装置STA1、STA2と平行して認証プロトコルを実行する能力を持つ不正通信者STA3が、通信装置STA1には不正通信者STA3通信装置（以下STA3は不正通信者又はその通信装置を意味する）が通信装置STA2であり、通信装置STA2には不正通信装置STA3が通信装置STA1であると信じさせることを目的とした攻撃方法である。

【0006】認証プロトコル「5. 2. 1 Two Pass Authentication」に対するMan in the Middle 攻撃は図8Aのようになる。不正通信装置STA3は、通信装置STA1から送られてきたメッセージを通信装置STA2へ送り、通信装置STA2から送られてきたメッセージを通信装置STA1へ送ることによって、上記目的を果たすことができる。

1：通信装置STA1はプロトコルをおこなう時点の時刻をT1とし、[T1, STA2]に対する署名S1を生成する。

2：通信装置STA1はその公開鍵PK1の証明書、T1, STA2, S1を不正通信装置STA3へ送る。（図8Aの1）

2a：不正通信装置STA3は通信装置STA1からの公開鍵PK1の証明書、T1, STA2, S1を通信装置STA2へ送る。（図8Aの2）

3：通信装置STA2は通信装置STA1からの証明書を用いて署名S1を検査する。

4：通信装置STA2はプロトコルをおこなう時点の時刻をT2とし、[T2, STA1]に対する署名S2を生成する。

5：通信装置STA2はその公開鍵の証明書、T2, STA1, S2を不正通信装置STA3へ送る。（図8Aの3）

5a：不正通信装置STA3は通信装置STA2からの公開鍵の証明書、T2, STA1, S2を通信装置STA1へ送る。（図8Aの4）

6：通信装置STA1は通信装置STA2からの証明書を用いて署名S2を検査する。

【0007】ここでは5. 2. 1 Two Pass Authentication について述べたが、5. 2. 2 Three Pass Authentication に対しても同じ攻撃を行うことができる。

・ Replay攻撃

不正通信者STA3が、通信装置STA2とSTA1の通信を傍受し、その情報を用いて、後の認証手順において通信装置STA2に不正通信装置STA3が通信装置STA1であると信じさせることを目的とした攻撃方法

である。

【0008】認証プロトコル「5. 2. 1 Two Pass Authentication」に対するReplay攻撃は図8Bのようになる。まず、通信装置STA1とSTA2の認証プロトコルが行われ、これを不正通信装置STA3が盗聴する。

1：通信装置STA1はプロトコルをおこなう時点の時刻をT1とし、[T1, STA2]に対する署名S1を生成する。

2：通信装置STA1はその公開鍵PK1の証明書、T1, STA2, S1を通信装置STA2へ送る。（図8Bの1）

3：通信装置STA2は通信装置STA1からの証明書を用いて署名S1を検査し、検査に不合格の場合はプロトコルを中断する。

4：通信装置STA2はプロトコルをおこなう時点の時刻をT2とし、[T2, STA1]に対する署名S2を生成する。

5：通信装置STA2はその公開鍵PK2の証明書、T2, STA1, S2を通信装置STA1へ送る。（図8Bの2）

6：通信装置STA1は通信装置STA2からの証明書を用いて署名S2を検査し、検査に不合格の場合はプロトコルを中断する。

【0009】つぎに通信装置STA1と（通信装置STA2であると偽った）不正通信装置STA3の認証プロトコルが行われる。

1：通信装置STA1はプロトコルをおこなう時点の時刻をT1'とし、[T1', STA2]に対する署名S1を生成する。

2：通信装置STA1はその公開鍵PK1の証明書、T1', STA2, S1を不正通信装置STA3へ送る。（図8Bの3）

3：不正通信装置STA3は通信装置STA1からの証明書を用いて署名S1を検査し、検査に不合格の場合はプロトコルを中断する。

4：不正通信装置STA3は先の盗聴により得た通信装置STA2の公開鍵PK2の証明書、T2, STA1, S2を通信装置STA1へ送る。（図8Bの4）

5：通信装置STA1は通信装置STA2の証明書を用いて署名S2を検査し、検査に不合格の場合はプロトコルを中断する。

【0010】不正通信装置STA3は、通信装置STA2が送ったのと同じメッセージを通信装置STA1へ送るため、不正通信装置STA3は前回の認証時と同じ時刻情報T2を使うことになり、通信装置STA1は不正通信装置STA3が通信装置STA2でないことを見破ることができる。鍵共有したあと、暗号化したメッセージを交換して認証を行うことにより、Replay攻撃を防ぐことは可能である。

【0011】しかし、不正通信者は、鍵共有プロトコルに対しても Man in the Middle攻撃を行うことにより、暗号化したメッセージを交換して認証を行う場合でも、なりすましをすることができる。また、

5. 2. 1 Two Pass Authentication

では、Replay攻撃に対する安全性を日時情報に依っているため、時刻情報を共有できない場合には完全ではなく、

5. 2. 2 Three Pass Authentication

では、メッセージのやりとりが1回増えて3回となるという問題がある。

【0012】

【発明が解決しようとする課題】この発明の目的は、証明書を交換する認証方法の、Man in the middle と呼ばれる攻撃方法に対する弱点を解決し、しかも認証用のメッセージの交換の回数を減らして効率化した、認証方法及びその装置を提供することにある。

【0013】

【課題を解決するための手段】この発明は、認証プロトコルの際に、証明書の交換に先だって交換される、鍵共有のための通信相手の装置が発生した乱数から算出された情報に対してデジタル署名を行うことを最も主要な特徴とする。従来技術とは、通信する両者が鍵共有を行う際に交換した情報を、認証プロトコルに用いる点が異なる。

【0014】

【発明の実施の形態】実施形態1_(請求項1)

図1Aに、この実施形態1を実施した場合の認証方法(プロトコル)のシーケンスを示す。

① 最初の1往復の信号の送受で通信装置STA1、STA2が各々発生した乱数A1、A2から算出された値 $G^{A1} \text{Mod } P$ 、 $G^{A2} \text{Mod } P$ をそれぞれ認証要求、認証要求付に付けて相手局に送ることにより交換し、Diffie-Hellman鍵配送アルゴリズムにより秘密鍵 K を $K = G^{A1} \cdot G^{A2} \text{Mod } P$ と算出して共有する。

【0015】なおG、PはDiffie-Hellman鍵配送アルゴリズムにおける公開鍵である。

② 共有して以降の信号の送受は、共有された秘密鍵 K を用いて暗号化されて行われる。したがって、鍵共有した当事者(STA1、STA2のいずれか)以外の第三者からの証明書の送信は、復号化処理により意味のないデータとなり、証明書の検証時に、排除することができる。以上により、証明書の送信者が、鍵共有を行った当事者であることが保証される。

③ 通信装置STA1は署名用鍵K1に対する公開鍵PK1の証明書と、Diffie-Hellman鍵配送アルゴリズムで用いた情報 $G^{A2} \text{Mod } P$ に対する署名用秘密鍵K1による署名を通信装置STA2へ送る。同様に通信装置STA2は署名用鍵K2に対する公開鍵PK2の証明書と、 $G^{A1} \text{Mod } P$ に対する署名用秘密鍵K2による署名を通信装

置STA1へ送る。

【0016】このようにしてセッション時に生成されて送受された情報：ここでは、鍵共有用の情報 $G^{A1} \text{Mod } P$ 、 $G^{A2} \text{Mod } P$ に対して、証明書中の公開鍵に対応する署名用鍵によってデジタル署名できる能力を示すことにより、自分が、証明書を傍受して、不正に流用している通信者ではなく、証明書に記載されている公開鍵の本物の所有者であることを示す。

【0017】つまり通信装置STA1は乱数を生成し、 $G^{A3} \text{Mod } P$ を演算し、認証要求と $G^{A3} \text{Mod } P$ を不正通信装置STA3へ送り、不正通信装置STA3は乱数A4を生成し、 $G^{A4} \text{Mod } P$ を演算し、これと認証要求受付とを通信装置STA1へ送る。両通信装置STA1、STA3はそれぞれ秘密鍵 $K' = G^{A3} \cdot G^{A4} \text{Mod } P$ を計算する。

【0018】次に共通した秘密鍵 K' で暗号化して送受信を行うが不正通信装置STA3は傍受した通信装置STA2の公開鍵PK2の証明書を用いてこれを通信装置STA1に送ることができるが、通信装置STA2のPK2と対応する署名用鍵K2を知らないため、 $G^{A1} \text{Mod } P$ に対する正しい署名を通信装置STA1へ送ることができない。

【0019】従って通信装置STA1は、公開鍵PK2が正しいものであることを確認することができるが、このPK2を用いて、不正通信装置STA3よりの $G^{A1} \text{Mod } P$ に対する署名と相当するものを検証した際に、不合格となり、秘密鍵 K' を共有した相手が通信装置STA2でないことが判明する。

④ 検証結果及び接続条件によって接続の可否を判断する。

【0020】上記により、鍵を共有した相手が証明書の送信者であり、かつ、証明書に記載されている公開鍵と対応する署名用鍵K1、K2を知っていることが相互に証明できる。この実施の形態において、Diffie-Hellman鍵配送アルゴリズムの代わりに、楕円Diffie-Hellman鍵配送アルゴリズムを使用することが可能である。

【0021】実施形態2_(請求項2)

公開鍵暗号(RSA暗号、ElGamal暗号、など)を用いて鍵A2を共有し、鍵A2を用いた暗号通信を行っている状態でデジタル署名を用いた認証プロトコルを行う場合を想定している。ここで、鍵共有に用いる公開鍵暗号の公開鍵にたいしても認証局が証明書を発行することにより、鍵共有と認証を同時に行う方法も考えられるが、

・鍵共有と署名用に別々の証明書を必要とする方式は、認証局の負担が増えること。

・認証プロトコルは暗号化した状態で行った方が不特定多数に認証用の情報が漏れる危険が減ること。

などの理由から、「鍵共有プロトコル」「暗号通信で認証プロトコル」という順に行うのが一般的である。

【0022】図2にこの実施形態の認証プロトコルのシーケンスを示す。

公開鍵暗号用の公開鍵PKとデジタル署名用の公開鍵PK1またはPK2は同じでも異なっても良いが、署名と暗号に同じ鍵を用いると、安全性に問題がある場合がある。

署名/暗号両用のアルゴリズムと比較して、どちらか片方しか出来ないアルゴリズムにより高速なものが存在する

という理由から、一般には異なる公開鍵を用いる。

① 最初の1往復の信号の送受で通信装置STA1は、通信装置STA2に通信装置STA1の公開鍵PKを認証要求と共に送信し、通信装置STA2は、乱数A2を発生し、公開鍵PKによって乱数A2を暗号化した値S2と認証要求受付を通信装置STA1に送り返す。

【0023】通信装置STA1はS2を復号して乱数A2を得る。以後、メッセージを暗号化する鍵としてA2を用いる。

② 共有して以降の信号の送受は、共有された鍵A2を用いて暗号化されて行われる。A2は、(a)発生した通信装置STA2と、(b)公開鍵PKに対応する秘密鍵SKを持っており、公開鍵PKによる暗号文を復号できる通信装置のみが知りえる情報である。

【0024】したがって、鍵共有した当事者(STA1, STA2のいずれか)以外の第三者からの証明書の送信は、復号化処理により意味のないデータとなり、証明書の検証時に、排除することができる。以上により、証明書の送信者が、鍵共有を行った当事者であることが保証される。

③ 通信装置STA1は、乱数A1を発生し、
・通信装置STA1の公開鍵PK1の証明書、
・通信装置STA1の秘密鍵K1による、 $[A1, S2]$ に対する署名
・A1, S2

を通信装置STA2に送る。

【0025】通信装置STA2は、
・通信装置STA2の公開鍵PK2の証明書
・通信装置STA2の秘密鍵K2による $[S2, A1]$ に対する署名
・S2, A1

を通信装置STA1に送る。

【0026】ここで、STA1→STA2のときと、STA2→STA1の時で、S2とA1の順番が逆になっているのは、従来法であるX5056-3(ISO/IEC9798-3)5.2.2 Three Pass Authenticationの該当する部分にならっている。両方とも同じ順番にしても良い。このような処理により、実施の形態1と同様、セッション時に生成されて送受された予測不可能な情報：ここでは、A1, S2を、証明書中の公開鍵に対応する署名用鍵によってデジタル署名できる能力を示

すことにより、自分が、証明書を傍受して、不正に流用している通信者ではなく、証明書に記載されている公開鍵の本物の所有者であることを示している。

④ 検証結果及び接続条件によって接続の可否を判断する。

【0027】上記により、鍵を共有した相手が証明書の送信者であり、かつ、証明書に記載されている公開鍵と対応する秘密鍵K1, K2を知っていることが相互に証明できる。この実施形態は、公開鍵暗号一般(RSA、ElGamal、楕円ElGamal、ラビン)による鍵配送方式に適用可能である。

【0028】実施形態1に用いられる通信装置STA1の機能構成例を図3に示す。記憶部11には乱数生成部ノイズ生成された乱数A1、鍵配送アルゴリズムに用いられる公開情報G, P、共有鍵生成部13で生成された共有鍵SK、その通信装置STA1の公開鍵PK1の証明書、そのPK1と対の署名用秘密鍵K1、相手通信装置STA2から送られた鍵配送用関数値結果G(A2)などが記憶されている。

【0029】関数演算部14では乱数A1、公開情報P, Gが入力されて鍵配送アルゴリズムによる鍵配送用関数F(A1)が演算される。つまり、鍵配送アルゴリズムは必ずしもDiffie-Hellmanのアルゴリズムに限らず、要は乱数A1を変数とした関数を利用するものであればよい。共有鍵生成部13では相手通信装置STA2からの鍵配送用関数値G(A2)と、乱数A1とから共有の秘密鍵SKを生成して、記憶部11に記憶する。

【0030】前記実施例ではG(A2)に対し、K1による署名を直接行ったが、G(A2)を変数とする関数H(G(A2))、例えばG(A2)を整数倍した簡単な関数や、複数次数の複雑な関数でもよい。更に乱数A1も付加したものでもよい。単純には $A1 + G(A2)$ 自体又は $H(A1 + G(A2))$ としてもよい。よってこの例では認証用演算部15でG(A2)とA1を変数として関数H(A1, G(A2))を演算し、その演算結果に対し、署名部16で、署名用秘密鍵K1によりデジタル署名がなされる。

【0031】その暗号部17では署名部16の署名結果、つまり認証用署名C1と、公開鍵PK1の証明書に対し、または検証結果生成部18からの検証結果に対し、共有鍵SKで暗号化する。認証要求と鍵配送用関数演算部14用演算結果F(A1)、や暗号部17の暗号化出力が送信部19により通信装置STA2など相手通信装置へ送信される。

【0032】通信装置STA2からなど外部からの信号が受信部20で受信され、それが認証要求受けの場合は、G(A2)が共有鍵生成部13へ入力され、共有鍵SKを生成以後の受信信号は復号部21で共有鍵SKで復号される。復号部21の出力中の公開鍵PK2の証明書に対し、公開鍵確認部22でその受信公開鍵PK2が

正しいものであることが確認され、その確認された公開鍵PK2を用いて、受信された認証用署名C2が署名検証部23で検証される。公開鍵確認部22、署名検証部23の各検証結果にもとづき、検証結果生成部18で検証結果が生成される。以上の各部に対する制御、その処理実行が制御部24により行われる。一般には、これらの処理はコンピュータにより行われる。

【0033】図4に図2に示した実施形態2の通信装置STA1の機能構成を図3と対応する部分に同一符号を付けて示す。この場合記憶部11には鍵配送用公開鍵 α （図2ではPK）、が鍵配送用公開情報P、Gの代りに記憶され、またG(A2)の代りに暗号情報G(α , A2) = S2が記憶される。鍵配送処理時には、記憶要求と鍵配送用公開鍵 α とが送信され、また受信部20で受信された鍵配送時の暗号情報G(α , A2)は共有鍵生成部13で公開鍵 α で復号され、前記実施例ではA2が共有鍵SKとされて記憶部11に記憶される。しかし、この共有鍵SKはA2の関数であればよい。また認証処理において、乱数生成部26から乱数A1を生成し、

(S2 = G(α , A2), A2) に対し直接署名用秘密鍵K1で署名したが、図3の場合と同様に認証用関数演算部15でH(A1, S2)を演算し、これに対し、署名部16でK1による署名を行ってもよい。その他は図3の場合と同一である。

【0034】この実施形態2における通信装置STA2の場合は図4に破線で示すように、鍵配送時に、乱数生成部27で乱数A2が生成され、その乱数A2に対し暗号部28で公開鍵 α により暗号化されG(α , A2)とされて送信される。共有鍵生成部ではA2と α から共有鍵SKが生成される。その他は通信装置STA1と同様である。通信装置STA1、STA2は何れが先に認証要求を出すかは不明であるから通信装置としては両機能を具備する。

【0035】図1乃至図4において共有鍵SKの生成後は、その共有鍵SKにより全ての送信情報と暗号化して送信し、受信情報をSKで復号すると述べたが、前記相互認証処理、つまり図1、図2に対する説明中の②、④においては共有鍵SKにより暗号化を行うことなく相互認証を行ってもよい。

【0036】

【発明の効果】この発明を実施すると、証明書の送信者が、証明書に記載されている公開鍵と対応する秘密鍵を知っていることの証明が行えるのと同時に、不正な第三者によるMan in the middle 攻撃の防止を、2-pathのメッセージ交換によって行うことができる。

【0037】この発明の実施形態1（図1）において、不正な第三者STA3がMan in the middle 攻撃を試みている状況を図5に示す。不正通信装置STA3は通信装置STA2に対しては通信装置STA1になりすまし、通信装置STA1に対しては通信装置STA2にな

りすますために、通信装置STA1からのメッセージを中継して通信装置STA2に送り、通信装置STA2からのメッセージを中継して通信装置STA1に送る。

【0038】この発明手順において、なりすましを実行するために、不正通信装置STA3は以下の①、②、③、④を行うことが必要である。鍵の共有のためのシーケンスの1番目と2番目のメッセージにおいては：

① 通信装置STA1にはF(A2)の代わりに自分で発生した乱数A3から関数Hによって算出されるH(A3)を送る。

② 通信装置STA2にはF(A2)の代わりに自分で発生した乱数A4から関数Iによって算出されるI(A4)を送る。

【0039】なお①と②を行わないで、F(A1)を通信装置STA2に、G(A2)を通信装置STA1に単に中継すると、通信装置STA1とSTA2は不正通信装置STA3には知りえない秘密鍵SKを共有出来ることになり、不正通信装置STA3が通信装置STA1、STA2になりすますることができない。認証の1-path目のシーケンスの3番目と4番目のメッセージにおいては：

③ 不正通信装置STA3は通信装置STA2が送信したG(A2)に対して、通信装置STA1のデジタル署名用鍵K1を用いてデジタル署名(Sig1)して通信装置STA2に、K1に対応する公開鍵PK1の証明書とともに送る。

④ 不正通信装置STA3は通信装置STA1が発生したF(A1)に対して、通信装置STA2のデジタル署名用鍵K2を用いてデジタル署名(Sig2)して通信装置STA1にK2に対応する公開鍵PK2の証明書とともに送る。

【0040】しかしながら、

(1) 不正通信装置STA3は証明書に記載されたデジタル署名用鍵K1、K2を知らない

(2) 通信装置STA1のところには、F(A2)は届かない

(3) 通信装置STA2のところにはF(A1)は届かない

ため、不正通信装置STA3にはSig1、Sig2を正しく偽造して送信することは不可能である。

【0041】次に、この発明の実施形態2（図2）において、不正な第三者STA3がMan in the middle 攻撃を試みている状況を図6に示す。この状況において、不正通信装置STA3が、通信装置STA1、STA2になりすますためには、鍵配送のために送受した、乱数A2、A3の通信装置STA1、STA3の公開鍵による署名S3、S2を、通信装置STA1、STA2の秘密鍵K1、K2を用いて署名できることが必要であるが、不正通信装置STA3はK1、K2を知らないで、これは不可能である。

【0042】上記により、この発明がMan in the middle 攻撃に対して有効であることが示せた。また、この発明は共有鍵による暗号通信が前提であって、その共有鍵の配送処理において利用した情報を相互認証に用いるため、メッセージの送信回数は2回で済み、効率的に認証を行うことができる。

【図面の簡単な説明】

【図1】この発明の実施例の認証プロトコルのシーケンスと不正な第三者STA3がReplay攻撃を試みている状況を示す図。

【図2】この発明を実施例2の認証プロトコルのシーケンスを示す図。

【図3】実施例1の通信装置の機能構成例を示すブロッ

ク図。

【図4】実施例2の通信装置の機能構成例を示すブロック図。

【図5】請求項1において、不正な第三者STA3がMan in the middle 攻撃を試みている状況を示す図。

【図6】本発明請求項4において、不正な第三者STA3がMan in the middle 攻撃を試みている状況を示す図。

【図7】AはTwo Pass Authentication の概要を示す図、BはThree Pass Authentication の概要を示す図である。

【図8】AはMan in the middle 攻撃の概要を示す図、BはReplay攻撃の概要を示す図である。

【図2】

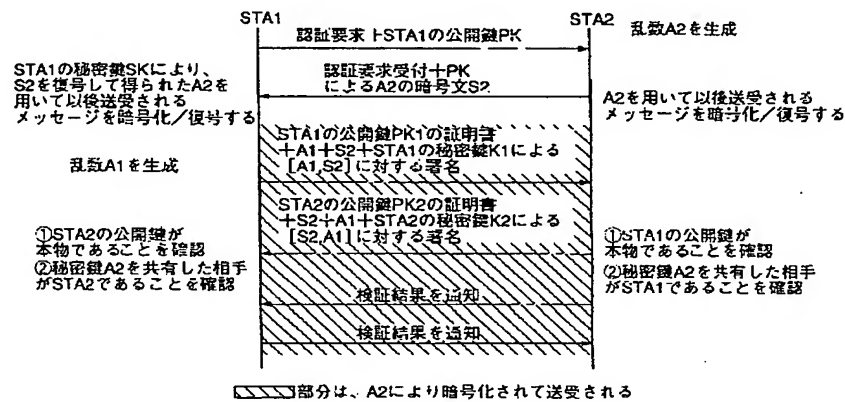


図 2

【図4】

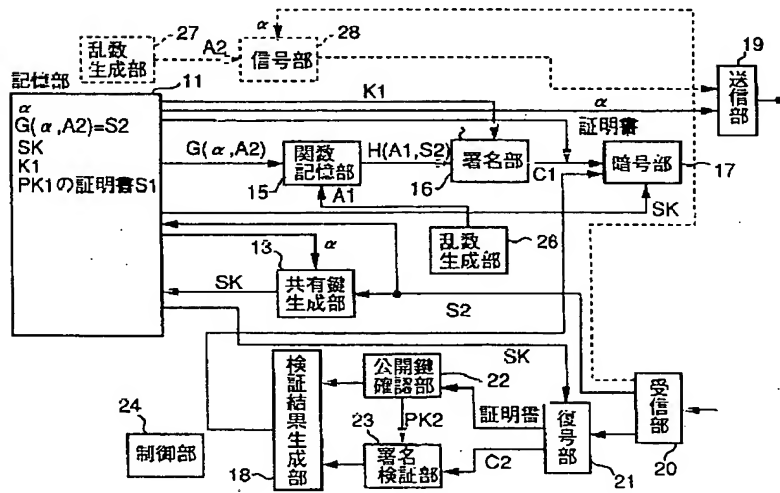
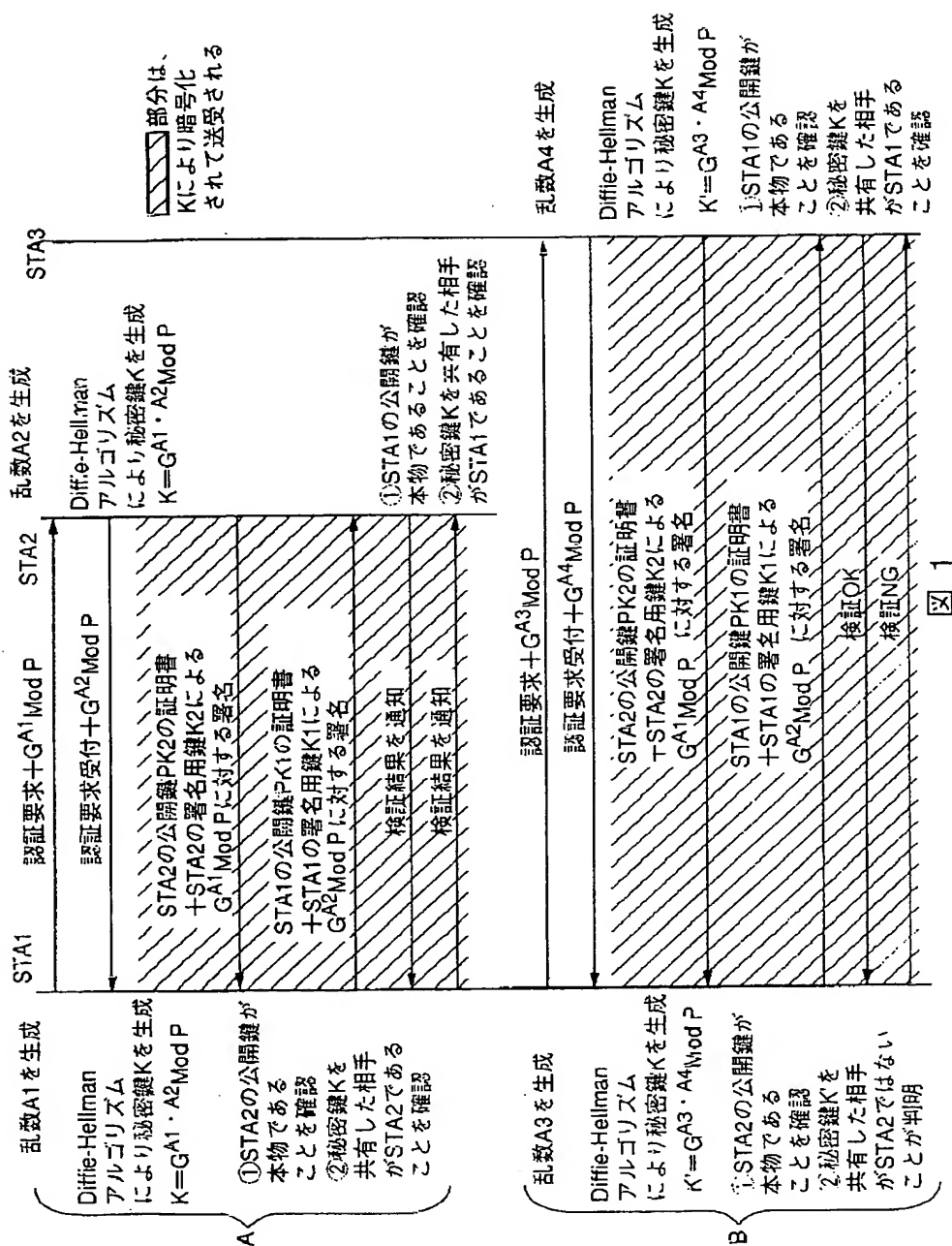


図 4

部分は、
Kにより暗号化
されて送受される



【図3】

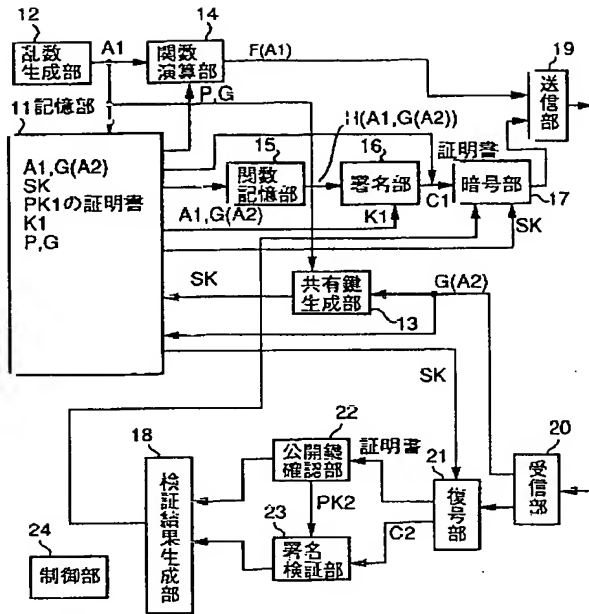


図 3

【図5】

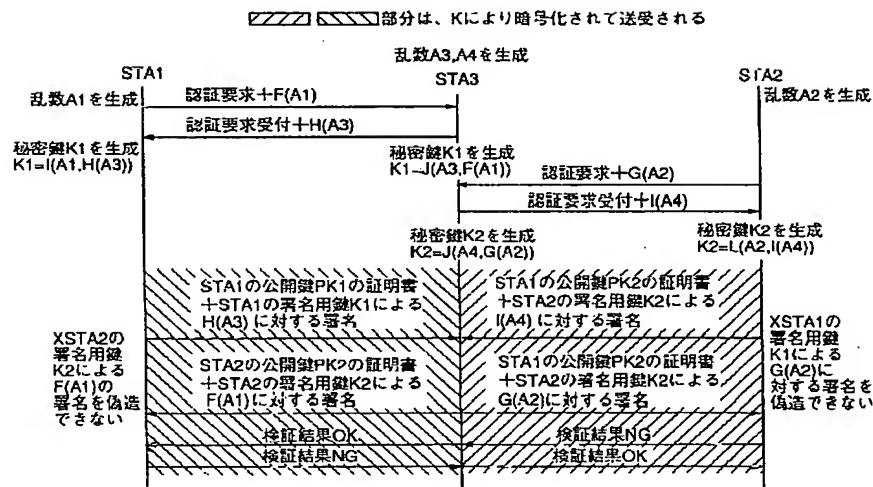


図 5

【図6】

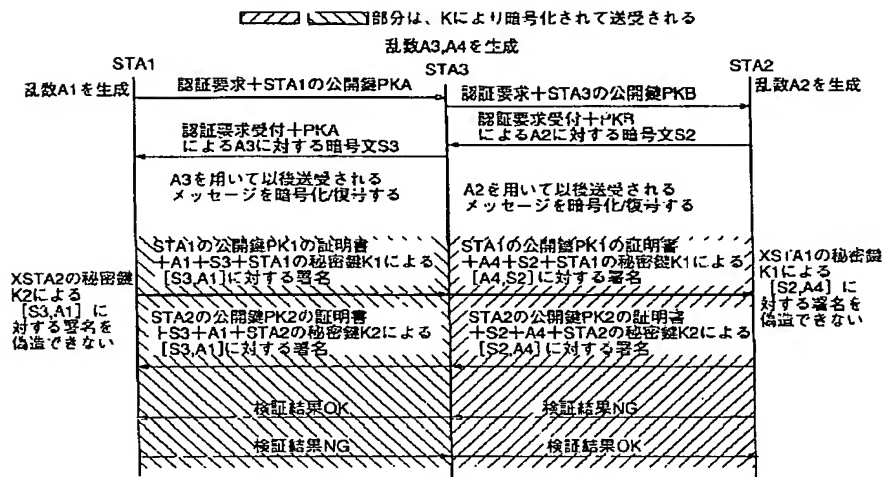


図 6

【図7】

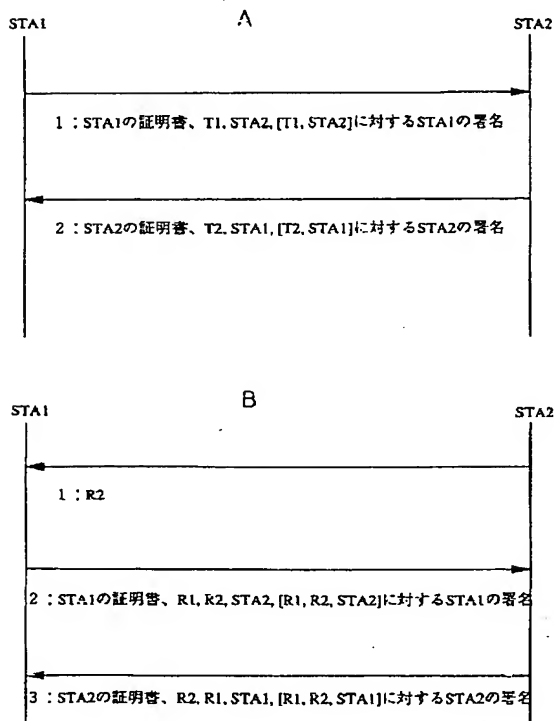


図 7

【図8】

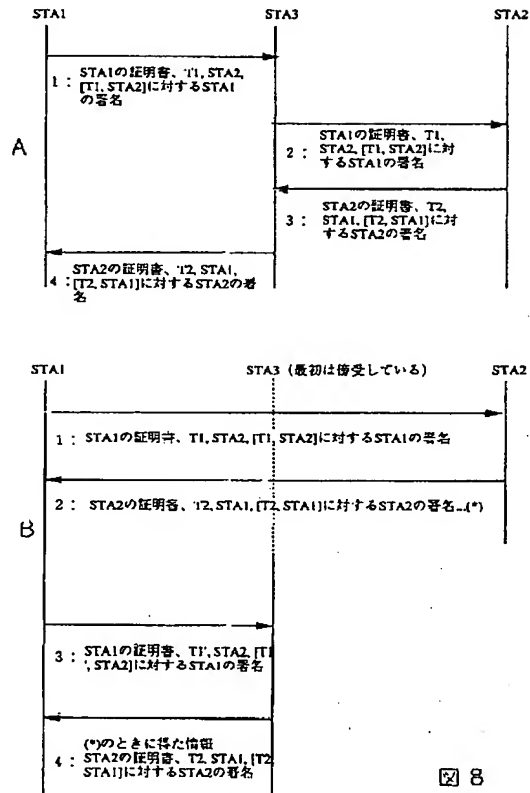


図 8